PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-259011
(43)Date of publication of application : 16.09.1994

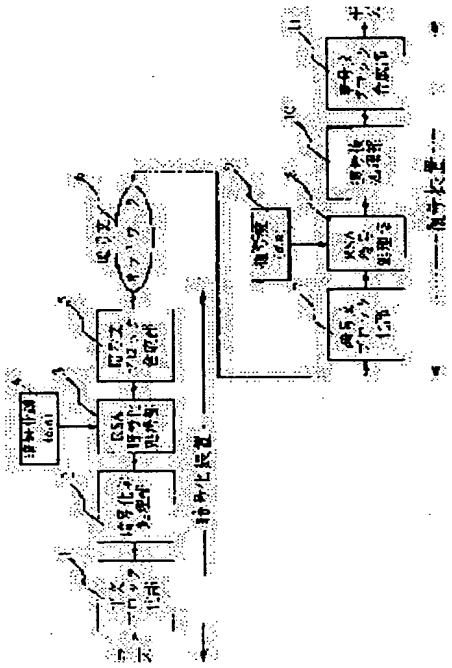
(51)Int.Cl. G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 05-042591
(22)Date of filing : 03.03.1993

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : ISHII SHINJI
MATSUMOTO HIROYUKI

(54) ENCIPHERING DEVICE AND DECODER FOR OPEN KEY

(57)Abstract:
PURPOSE: To make a ciphertext hard to be deciphered by excluding specific plaintexts 0, 1, and n-1 which become the same texts as the original plaintext even after RSA ciphering.
CONSTITUTION: A plaintext block division part 1 divides an input plaintext into plaintext blocks of integers between 0 and n-3, a enciphering preprocessing part 2 adds two to the respective plaintext blocks, and an RSA enciphering processing part 3 enciphers only blocks of integers between 2 and n-2 by utilizing an key (e, n). On a decoding side, an RSA decoding processing part 8 deciphers the respective ciphertext blocks by utilizing a decoding key (d, n), a decoding postprocessing part 10 substracts two from the decoding plaintexts, and the results are connected in order to obtain the original plaintext.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平６－２５９０１１

(43)公開日　平成６年（１９９４）９月１６日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
G09C 1/00		8837-5L		
H04L 9/06				
9/14				
		7117-5K	H04L 9/02	Z

審査請求　未請求　請求項の数２　ＯＬ　（全５頁）

(21)出願番号　特願平５－４２５９１

(22)出願日　平成５年（１９９３）３月３日

特許法第３０条第１項適用申請有り　１９９３年１月２２日、社団法人電子情報通信学会発行の「電子情報通信学会技術研究報告Ｖｏｌ．９２Ｎｏ．４３９」に発表

(71)出願人　０００００４２２６
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　石井　晋司
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　松本　博幸
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　草野　卓

(54)【発明の名称】公開鍵暗号化装置および復号装置

(57)【要約】　（修正有）
【目的】　ＲＳＡ暗号化しても元の平文と同一となる特定の平文０，１，ｎ－１を除外して、解読され難くする。
【構成】　平文ブロック化部１で入力平文を０以上ｎ－３以下の整数の平文ブロックに分割し、暗号化前処理部２でその各平文ブロックに２を加算して２以上ｎ－２以下の整数のブロックにつき、この各ブロックをＲＳＡ暗号化処理部３で鍵（ｅ，ｎ）を利用して暗号化する。復号側ではその各暗号文ブロックをＲＳＡ復号処理部８で復号鍵（ｄ，ｎ）を利用して復号し、その復号された各平文から２を復号後処理部１０で引算し、その結果を次に順次連続させて元の平文に戻す。

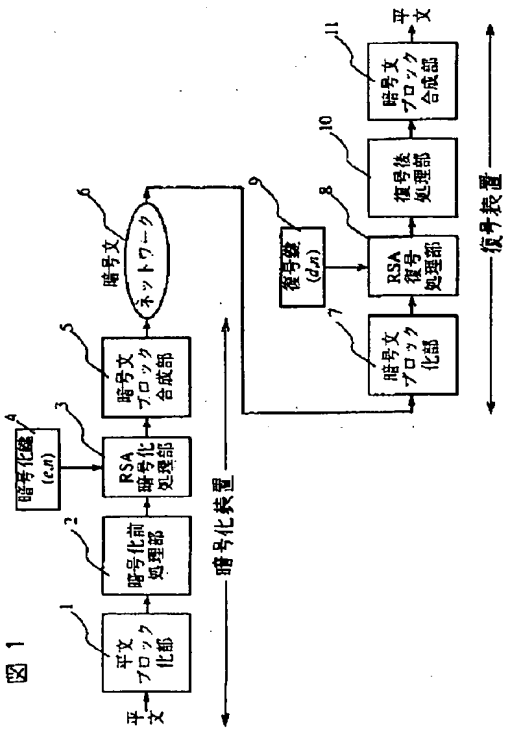


図１

1

【特許請求の範囲】

【請求項１】　冪乗および法ｎの剰余演算を利用する公開鍵暗号装置において、

０以上ｎ－３以下の整数で表現された平文に２を加える暗号化前処理手段と、

その暗号化前処理手段によって加算された平文２以上ｎ－２以下の整数で表現された暗号文に暗号化する平文暗号化手段と、

を具備する公開鍵暗号化装置。

【請求項２】　冪乗および法ｎの剰余演算を利用する公開鍵復号装置において、

２以上ｎ－２以下の整数で表現された暗号文を平文に戻す暗号文復号手段と、

その暗号文復号手段で復号された平文から２を引いて正規の平文を得る復号後処理手段と、

を具備する公開鍵復号装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、ＲＳＡ暗号で知られている冪（べき）乗および剰余演算を利用する公開鍵暗号アルゴリズムを利用する暗号化装置および復号装置に関するものである。

【０００２】

【従来の技術】冪乗および剰余演算を利用する公開鍵暗号アルゴリズムの代表として、ＲＳＡ暗号が知られている。（ＲＳＡ暗号の詳細な説明は、社団法人電子情報通信学会発行現代暗号理論第６章等を参照のこと）。ＲＳＡ暗号では、暗号化側が、暗号化指数ｅ、法ｎを利用して整数で表現された平文Ｍを暗号化する。一方復号側は、復号指数ｄ、法ｎを利用して暗号文Ｄをもとの平文Ｍに戻す。ＲＳＡ暗号は、アルゴリズムの特徴から、平文Ｍは、０≦Ｍ≦ｎ－１の整数に限られている。

【０００３】暗号化した結果が元の平文と一致する平文Ｍつまり暗号化できない平文Ｍが必ず９組あることが指摘されている（参考文献：社団法人電子情報通信学会発行現代暗号理論第６章ｐｐ．１１４－１１６）。しかし、従来は、実システムではｎは２の５１２乗程度であることから、前記９組が出現する確率は$9/2^{512}$と極めて小さいので特に重要視されていなかった。

【０００４】

【発明が解決しようとする課題】しかし、これらの９組中の３組は、特定の平文で、０，１，ｎ－１である。この０，１は暗号化指数ｅ、復号指数ｄ、法ｎに依存せず、ｎ－１は法ｎのみに従属な値である。したがって、どのような暗号化指数ｅ、復号指数ｄ、法ｎを選択したとしても、悪意を持つ盗聴者はこれらの３組の平文Ｍを、部分解読できる。

【０００５】たとえば、法ｎ以上の平文を暗号化する場合、ある図形や文字の書かれた資料をスキャナー（画像読み取り器）を使って２値データとして読み込むと、連

2

続した０が数キロビット続くこともしばしばある。このようなデータを、ＲＳＡ暗号を利用して暗号化しても、暗号文はもとの平文と全く同じ連続した０が数キロビットになってしまう。

【０００６】この発明の目的は、どのような鍵（暗号化指数ｅ、復号指数ｄ、法ｎ）を選んだとしても暗号化結果が必ず元の平文と同じになる組み合わせがない公開鍵暗号装置及びその復号装置を提供することにある。

【０００７】

【課題を解決するための手段】請求項１の発明によれば０以上ｎ－３以下の整数で表現された平文を補正定数加算手段により２が加算され、その加算された平文が平文暗号化手段で冪乗及び法ｎの剰余演算を利用して暗号化される。請求項２の発明によれば２以上ｎ－１以下の整数で表現された暗号文が暗号文復号手段で冪乗及び法ｎの剰余演算を利用して平文に復号され、補正定数減算手段によりその復号された平文から２が引算されて正規の平文とされる。

【０００８】

【作用】平文は０以上ｎ－３以下の整数で表現され、これに２が加算され、つまり平文は２以上ｎ－１の整数となり、この加算された平文が暗号化されるため、暗号化直前の平文には０，１は含まれない、つまり暗号化しても元の平文となる平文０と１は除外される。それだけ、暗号化しても元の平文となる特定平文の暗号化が避けられ、その特定平文の部分解読が避けられる。なお特定平文ｎ－１も除外して暗号化するには、最初に平文を０以上ｎ－４以下の整数で表現すればよい。

【０００９】

【実施例】この発明の実施例の概要を述べる。最初に、ｎ－３以上の整数を、あらかじめ０以上ｎ－４以下の複数個のデータブロックに分割する。このようにして、すべての正整数を０以上ｎ－４以下の整数に分割して、その後すべてのデータブロックに２を加える。つぎに、２以上ｎ－２以下のデータブロックに分割することにより、すべての正整数を特定平文を避けて暗号化できるようにする。

【００１０】この発明の暗号化装置および復号装置を用いた公開鍵暗号システムを図１に示す。この発明を実現するために従来装置に対して新たに加わる部分は、暗号化前処理部２と復号後処理部１０のみで、そのほかは従来のＲＳＡ暗号装置と全く同じである。なお、ディジタル信号は、通常２進数で表現するため、この実施例も２進数を前提として記述する。

【００１１】暗号化装置では暗号化しようとするデータ（平文）を平文ブロック化部１に入れる。平文ブロック化部１では、最初にデータを０以上ｎ－４以下のデータブロックに分割する。平文ブロック化部１の処理動作を図２を参照して説明する。まずｊを１とし（Ｓ１）、次に入力平文の先頭からｋビットを取り出してM_jとする

（S_7）。そのM_jがｎ－３より小さいかを調べ（S_8）、ｎ－３より小さければそのM_jをｊ番目の平文ブロックとする（S_9）。M_jがｎ－３より小でなければ、そのM_jの再下位ビットを残りの平文の先頭に戻し（S_{10}）、M_jを１ビット下位側（右側）にシフトし、つまり、M_jを２分の１として（S_{11}）、ステップS_9に移り、そのM_jをｊ番目の平文とする。次にｊを＋１してステップS_8に戻る（S_{12}）。

【００１２】このようにして得られた、０～ｎ－４の整数のｋビットの平文ブロックＭは、暗号化前処理部２でそのすべてのデータブロックに２を加え、図３Ａに示すように各平文ブロックＭの値２だけずらされる。これにより平文ブロックＭ（２≦Ｍ≦ｎ－２）が完成する。この平文ブロックＭは、従来のＲＳＡ暗号と同じ方法により、ＲＳＡ暗号化処理部３で暗号化鍵（ｅ，ｎ）を利用して暗号化し、暗号文Ｄ（２≦Ｄ≦ｎ－２）を得る。

【００１３】このとき暗号文Ｄのビット数は、２ビットからｋビットまで、ばらばらのビット長になる。データをこのまま複数の暗号文Ｄを連続して送信してしまうと、受信側では、どこが暗号文の切れ目であるかわからないために、復号できない。そこで、もっともビット長の長いｋビットにそろえるために、ｋビットに満たない暗号文には、ｋビットになるように上位ビットに０を加える。このようにすることにより、暗号文Ｄは、すべて、ｋビットの暗号文ブロックとなる。この暗号文ブロックは、ｋビットであるが、上位ビットに０が詰まっているだけであるので暗号文ブロックも暗号文Ｄと同じ暗号文ブロックＤ（２≦Ｄ≦ｎ－２）とあらわすことができる。

【００１４】暗号文ブロック合成部５では、暗号化データのビット長をｋビットに整え、暗号文ブロックＤとし、その暗号文ブロックＤを合成してネットワーク６を介して受信側に伝達する。受信側の復号装置は、受け取った暗号文を暗号文ブロック化部７に取込む。暗号文ブロック化部７では、受け取った暗号文をｋビットごとの暗号文ブロックに区切る。暗号文ブロックは、従来の復号と全く同じ方法で、ＲＳＡ復号処理部８で復号鍵（ｄ，ｎ）９を利用して復号する。

【００１５】つぎに、復号後処理部１０では、復号した平文ブロックから２を引き、図３Ｂに示すように整数２～ｎ－２をそれぞれ２だけ小さい値にずらす。最後に、平文ブロック合成部１１で平文ブロックを合成することにより元の平文に戻すことができる。補正定数の２は、盗聴者などに知られても、暗号強度には全く影響がない。したがって、補正定数は、誰もがいつでも２を使用しても何も問題はない。もちろん、暗号化側で、暗号文の送信の前に２をヘッダとして付与してたり、２を使用することを公開してもかまわない。上述では平文をまず０～ｎ－４の整数のブロックにしたが、平文を０～ｎ－３の整数のブロックに分割しても、通常はｎ－３の平文ブロックが連続するようなことはないから、これに２を加算したブロックはｎ－１で暗号文もｎ－１となるが、全体として解読されるおそれはない。

【００１６】

【発明の効果】従来の冪剰余を利用する公開鍵暗号アルゴリズムに共通した弱点の１つとして、どのような鍵を選んでも一部の暗号文は容易に解かれてしまう性質があった。しかしこの発明は、このような一部の暗号文をさけて暗号化することにより、どのような鍵を選んでも一部の暗号文が容易に解かれることを防ぐことができる。

【図面の簡単な説明】

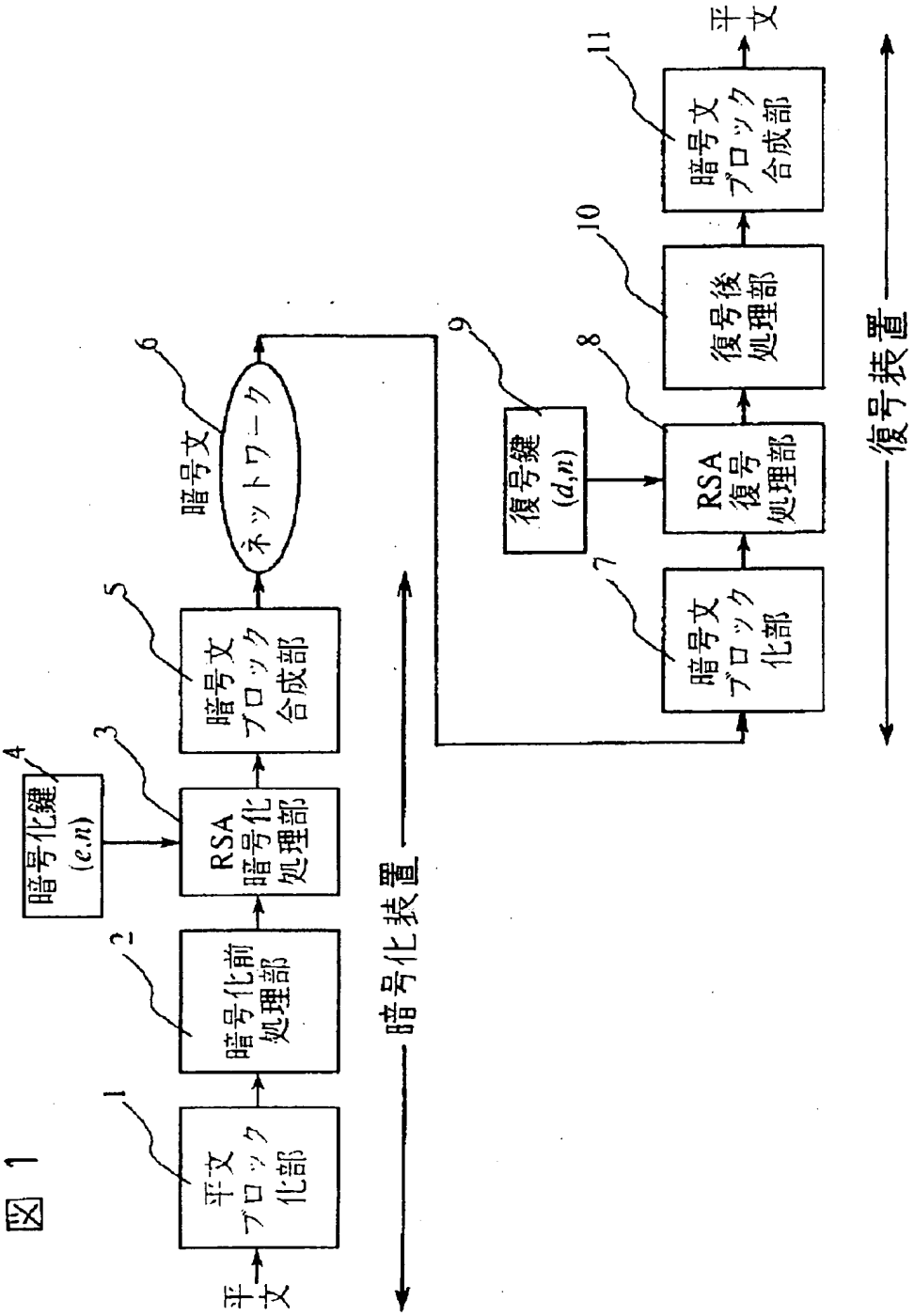
【図１】この発明の実施例の全体を示すブロック図。

【図２】十分長い平文をブロック化するための処理例を示す流れ図。

【図３】Ａは図１中の暗号化前処理部２の内部動作を具体的に説明する図、Ｂは図１中の復号後処理部１０の内部動作を具体的に説明する図である。

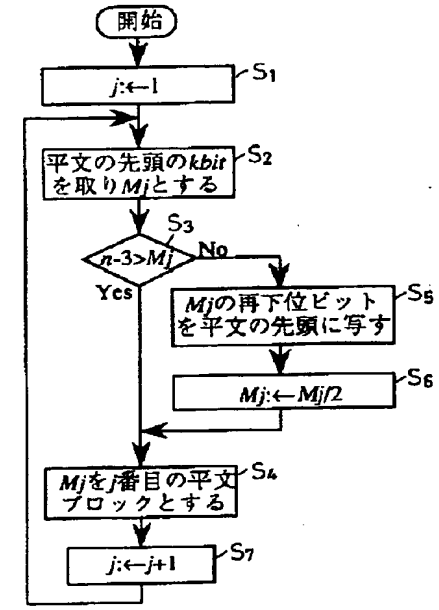
【図1】

図 1


平文
平文ブロック化部
1
暗号化前処理部
2
RSA暗号化処理部
3
暗号化鍵 (e,n)
4
暗号文ブロック合成部
5
暗号文
ネットワーク
6
暗号化装置
復号鍵 (d,n)
9
暗号文ブロック化部
7
RSA復号処理部
8
復号後処理部
10
暗号文ブロック合成部
11
平文
復号装置

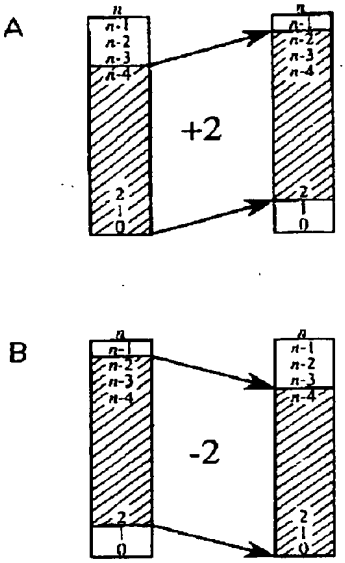
【図２】

図 2


開始
j:←1
S1
平文の先頭のkbitを取りMjとする
S2
S3
n-3>Mj
No
Yes
Mjの再下位ビットを平文の先頭に写す
S5
Mj:←Mj/2
S6
Mjをj番目の平文ブロックとする
S4
j:←j+1
S7

【図３】

図 3


A
+2
B
-2